Amendments to the Specification:

At page 6, lines 28-33, the following replacement paragraph is presented showing additions and deletions:

-- The key management module 52 receives the configuration parameter(s) and initializes a key management operation for a sender-receiver communication 58. For the embodiment where a key length parameter is received, at step 74, the key management module 52 derives an encryption key and returns the values 67 to the send configuration module 50 along the communication path 56. Where the configuration parameter includes the key, the key ~~es~~ is registered with the key management module by being stored. --

At page 7, line 27 to page 8 line 7, the following replacement paragraph is presented showing additions and deletions:

-- At step 86 the key management module 52 tests the access parameters (e.g., either default values or parameters registered by the send configuration module for the corresponding message identification ~~code.~~ code). When the access parameter is an expiration date and time, the current date time as defined by the computer hosting the key management module 52 is compared to the expiration date and time. When the access parameter defines a number of times the message is permitted to be decrypted, the key management module 52 tests a count which it maintains of the number of times a decryption key for the corresponding message has been given out. When the access parameter is a time period, the current time is compared to the time period. When the access parameter is for some other contingency, the contingency is evaluated. Examples of contingencies include but are not limited to: non-payment of funds, non receipt of subsequent messages. In another exemplary embodiment a contingency parameter is used to implement a subscription

mechanism such as for the sale or license of data. The key management module 52 implements the access parameters and promptly destroys decryption keys for messages that have expired or are otherwise no longer permitted to be accessed by the receiver. --

At page 8, lines 8-14, the following replacement paragraph is presented showing additions and deletions:

-- The testing at step 86 results in a decision at step 88 either allowing a decryption or disallowing a decryption. If a decryption is not allowed, then at step 90, the key management module 52 transmits a response 68 along communication path 62 to the receiver indicating that the decryption request has been denied. Accordingly, the decryption key is not ~~send~~ sent to the receiver module 54. If a decryption is allowed at decision step 88, then at step 92 the decryption key is sent to the receiver along communication path 62 as the response 68. --